

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-272561

(43)Date of publication of application : 08.10.1999

(51)Int.Cl.

G06F 12/14

G06F 3/06

(21)Application number : 10-068881

(71)Applicant : FUJITSU LTD

(22)Date of filing : 18.03.1998

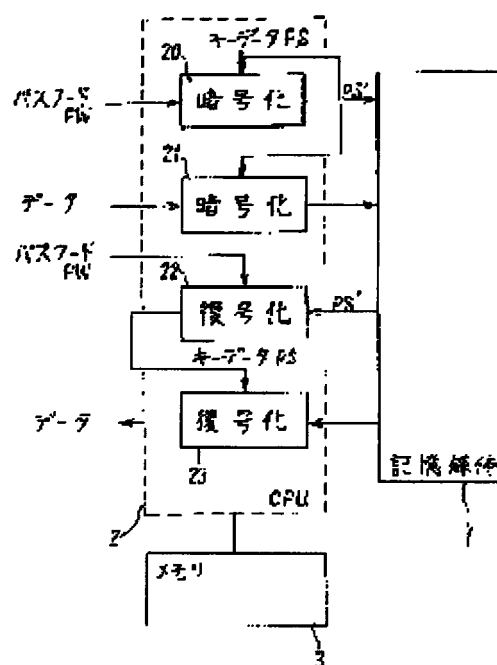
(72)Inventor : KOBAYASHI HIROYUKI
UCHIDA YOSHIAKI

(54) DATA PROTECTION METHOD FOR STORAGE MEDIUM DEVICE FOR THE SAME AND STORAGE MEDIUM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To change key data for each storage unit by one word in a data protection method for a storage medium and its device which encipher data to be recorded in the storage medium by a password and perform protection of the data.

SOLUTION: This device has a step which has a password PW encipher 20 key data P5 and writes them in a storage medium 1 after generating the key data P5 and a step which has the key data encipher 21 data and write them in the storage medium 1. Moreover, it has a step which reads the enciphered key data from the storage medium 1, a step which has the password decode 22 the enciphered key data, and a step which has the decoded key data decode 23 the data of the storage medium 1. Since enciphering is performed by using the key data generated separately from the password, an analysis of the password by decoding of a cryptogram is prevented.



LEGAL STATUS

[Date of request for examination]

01.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

【特許請求の範囲】

【請求項 1】 記憶媒体のデータを保護するための記憶媒体のデータ保護方法において、
 キーデータを生成して、前記キーデータをパスワードによって暗号化して、前記記憶媒体に書き込むステップと、
 前記キーデータによりデータを暗号化して、前記記憶媒体に書き込むステップと、
 前記記憶媒体から前記暗号化されたキーデータを読み出すステップと、
 前記暗号化されたキーデータを前記パスワードで復号化するステップと、
 前記復号化されたキーデータで前記記憶媒体のデータを復号化するステップとを有することを特徴とする記憶媒体のデータ保護方法。

【請求項 2】 請求項 1 の記憶媒体のデータ保護方法において、
 前記キーデータを生成するステップは、
 前記記憶媒体の論理セクタ毎に、前記キーデータを生成するステップであることを特徴とする記憶媒体のデータ保護方法。

【請求項 3】 請求項 2 の記憶媒体のデータ保護方法において、
 前記キーデータを生成するステップは、
 前記データの書き込み時に、前記論理セクタ毎に前記キーデータを生成するステップであることを特徴とする記憶媒体のデータ保護方法。

【請求項 4】 請求項 1 の記憶媒体のデータ保護方法において、
 前記キーデータを生成するステップは、予め定められた数のランダムデータを組み合わせ、前記キーデータを生成するステップであることを特徴とする記憶媒体のデータ保護方法。

【請求項 5】 請求項 1 の記憶媒体のデータ保護方法において、
 前記記憶媒体から前記暗号化されたキーデータを読み出した後、使用者が指定した旧パスワードにより復号化するステップと、
 前記復号化されたキーデータを、使用者が指定した新パスワードにより暗号化した後、前記記憶媒体に暗号化したキーデータを書き込むステップとを有することを特徴とする記憶媒体のデータ保護方法。

【請求項 6】 請求項 1 の記憶媒体のデータ保護方法において、
 前記暗号化されたキーデータを前記記憶媒体に書き込むステップは、
 複数のパスワードの各々で、前記キーデータを暗号化して、前記各暗号化されたキーデータを前記記憶媒体に書き込むステップであり、
 前記キーデータを復号化するステップは、

前記読み出した暗号化されたキーデータを指定されたパスワードで復号化するステップであることを特徴とする記憶媒体のデータ保護方法。

【請求項 7】 請求項 1 の記憶媒体のデータ保護方法において、
 前記暗号化されたキーデータを前記記憶媒体に書き込むステップは、
 一のパスワードで、前記キーデータを暗号化して、前記暗号化されたキーデータを前記記憶媒体に書き込み且つ一のパスワードで他のパスワードを暗号化して、暗号化された他のパスワードを書き込むステップであり、
 前記キーデータを復号化するステップは、
 前記暗号化された他のパスワードを前記他のパスワードで復号化して、前記一のパスワードを得るステップと、
 前記暗号化されたキーデータを前記一のパスワードで復号化するステップであることを特徴とする記憶媒体のデータ保護方法。

【請求項 8】 記憶媒体のデータを保護するための記憶媒体のデータ保護装置において、
 記憶媒体と、
 前記記憶媒体のデータをリード及びライトする制御回路とを有し、
 前記制御回路は、
 キーデータを生成した後、前記キーデータをパスワードによって暗号化して、前記記憶媒体に書き込み且つ前記キーデータによりデータを暗号化して、前記記憶媒体に書き込むライトモードと、
 前記記憶媒体から前記暗号化されたキーデータを読み出した後、前記暗号化されたキーデータを前記パスワードで復号化し、且つ前記復号化されたキーデータで前記記憶媒体のデータを復号化するリードモードとを有することを特徴とする記憶媒体のデータ保護装置。

【請求項 9】 請求項 8 の記憶媒体のデータ保護装置において、
 前記記憶媒体は、論理セクタ毎にリード／ライトされる記憶媒体で構成され、
 前記制御回路は、前記記憶媒体の論理セクタ毎に、前記キーデータを生成することを特徴とする記憶媒体のデータ保護装置。

【請求項 10】 請求項 9 の記憶媒体のデータ保護装置において、
 前記制御回路は、前記データの書き込み時に、前記論理セクタ毎に前記キーデータを生成することを特徴とする記憶媒体のデータ保護装置。

【請求項 11】 請求項 8 の記憶媒体のデータ保護装置において、
 前記制御回路は、予め定められた数のランダムデータを組み合わせ、前記キーデータを生成することを特徴とする記憶媒体のデータ保護装置。

【請求項 12】 請求項 8 の記憶媒体のデータ保護装置

において、
前記制御回路は、
前記記憶媒体から前記暗号化されたキーデータを読み出した後、使用者が指定した旧パスワードにより復号化し、且つ前記復号化されたキーデータを、使用者が指定した新パスワードにより暗号化した後、前記記憶媒体に暗号化したキーデータを書き込むことを特徴とする記憶媒体のデータ保護装置。

【請求項13】 請求項8の記憶媒体のデータ保護装置において、
前記制御回路は、
複数のパスワードの各々で、前記キーデータを暗号化して、前記各暗号化されたキーデータを前記記憶媒体に書き込むライトモードと、
前記読みだした暗号化されたキーデータを指定されたパスワードで復号化するリードモードとを有することを特徴とする記憶媒体のデータ保護装置。

【請求項14】 請求項8の記憶媒体のデータ保護装置において、
前記制御回路は、
一のパスワードで、前記キーデータを暗号化して、前記暗号化されたキーデータを前記記憶媒体に書き込み且つ一のパスワードで他のパスワードを暗号化して、暗号化された他のパスワードを書き込むライトモードと、
前記暗号化された他のパスワードを前記他のパスワードで復号化して、前記一のパスワードを得た後、前記暗号化されたキーデータを前記一のパスワードで復号化するリードモードとを有することを特徴とする記憶媒体のデータ保護装置。

【請求項15】 保護されたデータを有する記憶媒体において、
パスワードによって暗号化されたキーデータと、
前記キーデータによって暗号化されたデータとを有することを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報処理機器において、記憶媒体に記録するデータをパスワードにより暗号化して、データの保護を行うための記憶媒体のデータ保護方法、その装置及びその記憶媒体に関する。

【0002】 光ディスク、磁気ディスク、ICカード等を利用した記憶装置は、コンピュータ、ワードプロセッサ、電子ブック等の様々な情報処理機器に利用されている。この記憶装置では、プライバシーに係わる情報や職務上の機密情報など、本来所有者以外に知られたくない情報が書き込まれることがある。このような情報を他人に知られないようにするため、データを暗号化することが必要となる。

【0003】

【従来の技術】 図15は、従来技術の説明図である。

【0004】 光ディスク等の記憶媒体90又は記憶装置に対し、パスワードを設定する。データの書き込みに際しては、暗号化部91によりデータをパスワードで暗号化して、記憶媒体90に書き込む。又、読み出し時には、復号化部92により記憶媒体90のデータをパスワードで復号化する。

【0005】 このように、データを暗号化することにより、データの秘匿を行うことができる。この場合に、従来、記憶媒体全体に1つのパスワードを設定する方式であった。又、記憶媒体のファイル単位に異なるパスワードを設定する方式もある。

【0006】

【発明が解決しようとする課題】 しかしながら、従来技術では、次の問題があった。

【0007】 第1に、サンプルとしての暗号文又は暗号文と暗号化されていない平文の組み合わせが多い程、解読者の解読が容易となる。同一の平文を同一のパスワードで暗号化した結果は、等しいので、同一のパスワードで直接暗号化した場合には、暗号文の統計的性質は、平文の統計的性質を反映する。従って、従来の記憶媒体を同一のパスワードで暗号化する方式では、暗号文が統計処理できる程多量にあれば、平文の性質を容易に推定できるという問題があった。

【0008】 第2に、光ディスク等の大容量記憶媒体に保存されているデータには、そのディレクトリ部分などの定型フォーマットで構成されている部分がある。従来の記憶媒体を同一のパスワードで暗号化する方式では、このような部分を解析することにより、パスワードを推定すると、他の重要なデータも解読されてしまうという問題があった。

【0009】 第3に、従来のファイル毎に、パスワードを設定する方式では、一部分のパスワードの解読により、他の部分の解読を防止できる。しかし、この場合、ファイル毎に、異なるパスワードを管理する必要がある。このため、煩雑であり、パスワード忘却等の事故を招きやすいという問題があった。

【0010】 第4に、光ディスク等の交換可能な大容量記憶媒体においては、記憶媒体を持ち出したり、記憶媒体を複製することが可能である。このため、一旦暗号化されたデータを持ち出し、ゆっくりと解析することが可能である。従って、暗号文からパスワードを推定しやすいという問題もあった。

【0011】 第5に、従来は、パスワードで直接暗号化していたため、パスワードを変えると、データ全体を再暗号化する必要があるという問題もあった。

【0012】 本発明の目的は、暗号文からパスワードが解析されにくい記憶媒体のデータ保護方法、その装置及びその記憶媒体を提供することにある。

【0013】 本発明の他の目的は、一つのパスワードで、各記憶単位に、キーデータを変えることができる記

憶媒体のデータ保護方法、その装置及びその記憶媒体を提供することにある。

【0014】本発明の更に他の目的は、パスワードを変えても、データの再暗号化を不要とする記憶媒体のデータ保護方法、その装置及びその記憶媒体を提供することにある。

【0015】

【課題を解決するための手段】本発明の記憶媒体のデータ保護方法は、キーデータを生成した後、前記キーデータをパスワードによって暗号化して、前記記憶媒体に書き込むステップと、キーデータによりデータを暗号化して、前記記憶媒体に書き込むステップとを有する書き込みモードを有する。そして、そのデータ保護方法は、記憶媒体から前記暗号化されたキーデータを読み出すステップと、暗号化されたキーデータを前記パスワードで復号化するステップと、復号化されたキーデータで前記記憶媒体のデータを復号化するステップとを有するリードモードとを有する。

【0016】本発明では、パスワードをそのまま暗号化キーとして用いるのではなく、パスワードとは、別に生成したキーデータを用いて、データを暗号化する。キーデータは、パスワードをキーとして暗号化して、記憶媒体に書き込む。読み出し時には、パスワードにより、暗号化されたキーデータを復号化して、キーデータを得る。そして、キーデータでデータを復号化する。

【0017】このようにパスワードとは、別に生成したキーデータを用いて、データを暗号化することにより、暗号文を解析しても、暗号化されたキーデータが読解されるだけである。このため、パスワードやキーデータを解析しにくい。これにより、暗号文の解析によるパスワードの読解を防止できる。

【0018】又、パスワードとは、別に生成したキーデータを用いて、暗号化するため、1つのパスワードに対し、キーデータを変えることにより、セクタ等の記憶単位に異なるキーを付与できる。このため、論理セクタ毎に異なるキーを用いて、暗号化でき、データの機密性を高めることができる。

【0019】更に、パスワードとは、別に生成したキーデータを用いて、暗号化するため、パスワードを変えても、データの再暗号化が不要となる。このため、数百メガバイトの大容量記憶媒体でも、容易にパスワードの変更を実現できる。

【0020】

【発明の実施の形態】図1は、本発明の一実施の形態のブロック図、図2は、本発明の第1の実施の形態の論理フォーマット時の処理フロー図、図3は、本発明の第1の実施の形態の書き込み処理フロー図、図4は、本発明の第1の実施の形態の記憶領域の説明図、図5は、本発明の第1の実施の形態のキーデータの説明図、図6は、本発明の第1の実施の形態の読み出し処理フロー図であ

る。

【0021】図1に示すように、記憶媒体1は、光磁気ディスクで構成されている。この記憶媒体1の論理セクタサイズを、2KB（キロバイト）とする。制御回路2は、プロセッサで構成されている。第1の暗号化部20は、キーデータPSを使用者が入力したパスワードPWにより暗号化し、且つ暗号化したキーデータPS'を記憶媒体1に書き込む。

【0022】第2の暗号化部21は、書き込むべきデータをキーデータPSで暗号化し、暗号化されたデータを記憶媒体1に書き込む。第1の復号化部22は、記憶媒体1の暗号化されたキーデータPS'を、使用者が入力したパスワードPWで復号化する。第2の復号化部23は、復号化されたキーデータPSにより、記憶媒体1のデータを復号化して、データを出力する。メモリ3は、制御回路（以下、CPUという）2の作業域を与えるものである。尚、第1、第2の暗号化部20、21、第1、第2の復号化部22、23は、CPU2の処理をブロックにして示したものである。

【0023】図2により、媒体の論理フォーマット作成時の処理について、説明する。媒体の初期処理である媒体の論理フォーマット作成時に、以下の処理を実行する。

【0024】（S1）使用者は、ユーザーパスワードPWをCPU2に入力する。

【0025】（S2）CPU2は、セクタ数分の乱数（8バイト）を発生する。この乱数が、キーデータPSである。以下、セクタ数をnとし、PS[1]～PS[n]の乱数を生成したものと説明する。

【0026】（S3）CPU2は、このセクタ数分の乱数（ランダムデータ）PS[]（PS[1]～PS[n]）を、メモリ3の作業域に格納する。

【0027】（S4）CPU2は、作業域のキーデータPS[1]～PS[n]の各々を、パスワードPWで暗号化する。もちろん、作業域のキーデータPS[1]～PS[n]の全体をパスワードPWで暗号化しても構わない。

【0028】（S5）CPU2は、暗号化されたキーデータPS'[1]～PS'[n]を記憶媒体1の領域L1に書き込む。

【0029】図4に示すように、記憶媒体（ディスク）1の論理フォーマットは、各セクタで示される。このセクタは、論理ブロックアドレスLBAによりアドレスされる。ここで、図では、LBAが、「1」から「X」までX個のセクタが設けられている。

【0030】この光ディスクの記憶領域の内、先頭セクタ（LBA=1）からaセクタ分の領域L1を、暗号化されたキーデータPS'[1]～PS'[n]の格納領域に割り当てる。即ち、データの使用域のセクタ数は、n（=（X-a））であり、各使用域のセクタ毎に、領

域L1に、暗号化されたキーデータPS'〔1〕～PS'〔n〕が格納される。

【0031】次に、媒体の書き込み処理について、図3により説明する。

【0032】(S10) 論理ブロックアドレス(セクタ番号) LBAが、「S0」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0033】(S11) CPU2は、光ディスク1の領域L1のデータ(暗号化されたキーデータ)を読み出し済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS14に進む。

【0034】(S12) CPU2は、領域L1のデータを読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域L1のデータPS'〔1〕～PS'〔n〕を読み出す。

【0035】(S13) CPU2は、領域L1のデータPS'〔1〕～PS'〔n〕を、パスワードPWで復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔 〕 (PS〔1〕～PS〔n〕)を、メモリ3の作業域に格納する。

【0036】(S14) CPU2は、メモリ3の作業域のキーデータから、論理ブロックアドレス(セクタ番号) LBA(=S0)のキーデータPS〔S0〕を得る。図5に示すように、メモリ3の作業域のキーデータテーブルから論理ブロックアドレスLBAに対応するキーデータPS〔S0〕が得られる。そして、CPU2は、書き込むべきデータを、このキーデータPS〔S0〕で暗号化する。暗号化の方法としては、周知のDES等を用いることができる。

【0037】(S15) CPU2は、この暗号化されたデータを、光ディスク1の論理ブロックアドレスLBA(=S1)の位置に書き込む。

【0038】次に、図6を用いて、読み出し処理を説明する。

【0039】(S20) 論理ブロックアドレス(セクタ番号) LBAが「S0」の位置への読み出し要求が生じたとする。読み出し要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0040】(S21) CPU2は、光ディスク1の領域L1のデータ(暗号化されたキーデータ)を読み出し

済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS24に進む。

【0041】(S22) CPU2は、領域L1のデータを読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域L1のデータPS'〔1〕～PS'〔n〕を読み出す。

【0042】(S23) CPU2は、領域L1のデータPS'〔1〕～PS'〔n〕を、パスワードPWで復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔 〕 (PS〔1〕～PS〔n〕)を、メモリ3の作業域に格納する。

【0043】(S24) CPU2は、メモリ3の作業域のキーデータから、論理ブロックアドレス(セクタ番号) LBA(=S0)のキーデータPS〔S0〕を得る。図5に示すように、メモリ3の作業域のキーデータテーブルから論理ブロックアドレスLBAに対応するキーデータPS〔S0〕が得られる。そして、CPU2は、論理ブロックアドレスS1のデータを、光ディスク1から読み出す。更に、CPU2は、読み出したデータをキーデータPS〔S0〕で復号化する。復号化の方法としては、周知のDES等を用いることができる。復号化されたデータを要求元(例えば、コンピュータ)に送り出す。

【0044】このようにして、媒体の論理フォーマット作成時に、論理セクタ毎に、乱数を発生して、論理セクタ毎のキーデータを生成する。そして、記憶媒体1に、パスワードで暗号化されたキーデータを書き込んでおく。データの書き込み時には、キーデータによりデータを暗号化して、記憶媒体1に書き込む。

【0045】データの読み取り時には、記憶媒体1の暗号化されたキーデータを読み出した後、パスワードで復号化して、キーデータを得る。そして、記憶媒体から読み出したデータを、このキーデータにより復号化する。

【0046】このように、パスワードとは別に生成したキーデータにより、データを暗号化することにより、暗号文を解析しても、暗号化されたキーデータが解読されるだけである。このため、パスワードやキーデータを解析しにくい。これにより、暗号文の解析によるパスワードの解読を防止できる。

【0047】又、パスワードとは、別に生成したキーデータを用いて、暗号化するため、1つのパスワードに対し、キーデータを変えることにより、論理セクタ単位に異なるキーを付与できる。このため、論理セクタ毎に異なるキーを用いて、暗号化でき、データの機密性を高めることができる。

【0048】尚、領域L1を論理ブロックアドレスの小さい方に設けているが、領域L1を論理ブロックアドレ

スの最大の部分に格納しても良い。

【0049】図7は、本発明の第2の実施の形態の書き込み処理フロー図である。図7により、媒体の書き込み処理について、説明する。媒体の論理フォーマット作成時の処理は、図2の実施の形態と同様に行い、記憶媒体1に各論理セクタの暗号化されたキーデータを格納しておく。

【0050】(S30) 論理ブロックアドレス(セクタ番号) LBAが「S0」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、
10 「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0051】(S31) CPU2は、光ディスク1の領域L1のデータ(暗号化されたキーデータ)を読み出し済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS34に進む。

【0052】(S32) CPU2は、領域L1のデータ
20 が読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域L1のデータPS'〔1〕～PS'〔n〕を読み出す。

【0053】(S33) CPU2は、領域L1のデータPS'〔1〕～PS'〔n〕を、パスワードPWで復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔 〕 (PS〔1〕～PS〔n〕) を、メモリ3の作業域に格納する。
30

【0054】(S34) CPU2は、乱数Rを発生する。そして、CPU2は、メモリ3の作業域のキーデータの論理ブロックアドレス(セクタ番号) LBA(=S0)のキーデータPS〔S0〕に、乱数Rを書き込む。

【0055】(S35) そして、CPU2は、書き込むべきデータを、このキーデータPS〔S0〕(乱数R)で暗号化する。暗号化の方法としては、周知のDES等を用いることができる。CPU2は、この暗号化されたデータを、光ディスク1の論理ブロックアドレスLBA(=S1)の位置に書き込む。
40

【0056】(S36) CPU2は、適当なタイミングで、光ディスク1の領域L1のデータを書き換える。即ち、CPU2は、書き込み回数を示す書き込みカウンタの値WCが、例えば、32回を越えた場合には、安全のため、領域L1を書き換えるため、ステップS37に進む。一定回数毎に書き込むのは、何らかの異常により媒体排出等の処理がなされない事態が生じて、ある程度のデータ回復を保証するためのものである。32回という数値は任意である。この処理は本発明の必須要件ではない。又、CPU2は、記憶媒体1の排出要求があった
50

場合に、キーデータを保存するため、ステップS37に進む。更に、CPU2は、電源のオフが生じた場合に、キーデータを保存するため、ステップS37に進む。

【0057】(S37) CPU2は、作業域のキーデータPS〔1〕～PS〔n〕の各々を、パスワードPWで暗号化する。もちろん、作業域のキーデータPS〔1〕～PS〔n〕の全体をパスワードPWで暗号化しても構わない。次に、CPU2は、暗号化されたキーデータPS'〔1〕～PS'〔n〕を記憶媒体1の領域L1に書き込む。

【0058】この第2の実施の態様では、第1の実施の形態の作用に加えて、データの書き込み毎に、異なるキーデータを生成する。このため、データの書き込み毎に、異なるキーデータで暗号化され、データの秘匿性が向上する。

【0059】尚、読み出し処理は、図6の第1の実施の形態と同一であるので、説明を省略する。

【0060】図8は、本発明の第3の実施の形態の書き込み処理フロー図、図9は、本発明の第3の実施の形態のキーデータの説明図、図10は、本発明の第3の実施の形態の読み出し処理フロー図である。

【0061】媒体の論理フォーマット時には、図2で示した第1の実施の形態と同様にして、光ディスク1の領域L1に、暗号化されたキーデータPS'〔1〕～PS'〔512〕を格納する。但し、ここでは、各論理セクタ毎に、暗号化されたキーデータを格納しない。例えば、領域L1の大きさを4KBとする。そして、パスワードを8バイト/エントリとすると、図9に示すように、512個(エントリ)のキーワードPS〔1〕～PS〔512〕を生成する。そして、領域L1には、512個の暗号化されたキーワードPS'〔1〕～PS'〔512〕を格納する。

【0062】図8により、書き込み処理について、説明する。

【0063】(S40) 論理ブロックアドレス(セクタ番号) LBAが「S0」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、
「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。
40

【0064】(S41) CPU2は、光ディスク1の領域L1のデータ(暗号化されたキーデータ)を読み出し済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS44に進む。

【0065】(S42) CPU2は、領域L1のデータが読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域
50

L1のデータPS'[1]~PS'[n]を読みだす。

【0066】(S43)CPU2は、領域L1のデータPS'[1]~PS'[n]を、パスワードPWで復号化する。これにより、キーデータPS[1]~PS[n]が得られる。このキーデータPS[](PS[1]~PS[n])を、メモリ3の作業域に格納する。

【0067】(S44)CPU2は、要求されたセクタ番号S0から4つの値R0、R1、R2、R3を得る。ここでは、論理セクタ番号S0を32ビットのビット列と見なし、8ビットづつを1つの値R0、R1、R2、R3に纏める。R0~R3は、0以上256未満の値になる。そして、R0~R3をインデックスとして、メモリ3の作業域のPS[]から乱数値(キーデータ)を取り出す。取り出した4つの値を基に、8バイトの乱数(キーデータ)Rを発生する。

【0068】ここでは、図9に示すように、R0に対応するキーデータPS[R0]を取り出し、(R1+256)に対応するキーデータPS[R1+256]を取り出す。R2に対応するキーデータPS[R2+256]を取り出し、R3に対応するキーデータPS[R3]を取り出す。

【0069】そして、下記演算式により、キーデータRを演算する。

【0070】

$$R = (PS[R0] * PS[R1 + 256]) * (PS[R2 + 256] + PS[R3])$$

尚、「*」は、EOR演算である。

【0071】(S45)そして、CPU2は、書き込むべきデータを、このキーデータRで暗号化する。暗号化の方法としては、周知のDES等を用いることができる。CPU2は、この暗号化されたデータを、光ディスク1の論理ブロックアドレスLBA(=S1)の位置に書き込む。

【0072】次に、図10により、読み出し処理を説明する。

【0073】(S50)論理ブロックアドレス(セクタ番号)LBAが「S0」の位置への読み出し要求が生じたとする。読み出し要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0074】(S51)CPU2は、光ディスク1の領域L1のデータ(暗号化されたキーデータ)を読み出し済かを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS54に進む。

【0075】(S52)CPU2は、領域L1のデータが読み出し済でないなら、メモリ3の作業域に、キーデ

ータを展開する処理を行う。即ち、CPU2は、ユーザーパスワードPWを得る。そして、光ディスク1の領域L1のデータPS'[1]~PS'[n]を読みだす。

【0076】(S53)CPU2は、領域L1のデータPS'[1]~PS'[n]を、パスワードPWで復号化する。これにより、キーデータPS[1]~PS[n]が得られる。このキーデータPS[](PS[1]~PS[n])を、メモリ3の作業域に格納する。

【0077】(S54)CPU2は、要求されたセクタ番号S0から4つの値R0、R1、R2、R3を得る。論理セクタ番号S0を32ビットのビット列と見なし、8ビットづつを1つの値R0、R1、R2、R3に纏める。そして、R0~R3をインデックスとして、メモリ3の作業域のPS[]から乱数値(キーデータ)を取り出す。取り出した4つの値を基に、8バイトの乱数(キーデータ)Rを発生する。

【0078】ここでは、図9に示すように、R0に対応するキーデータPS[R0]を取り出し、(R1+256)に対応するキーデータPS[R1+256]を取り出す。R2に対応するキーデータPS[R2+256]を取り出し、R3に対応するキーデータPS[R3]を取り出す。

【0079】そして、上述した演算式より、キーデータRを演算する。

【0080】(S55)そして、CPU2は、光ディスク1から論理ブロックアドレスLBA(=S1)のデータを読みだす。更に、読みだしたデータを、このキーデータRで復号化する。復号化の方法としては、周知のDES等を用いることができる。

【0081】この第3の実施の形態では、第1の実施の形態に比し、光ディスク1の領域L1の大きさを小さくできる。即ち、第1の実施の形態では、論理セクタの数と同数のキーデータを格納する必要がある。例えば、1セクタを2KBとし、記憶容量を600MBとし、キーデータを8Byteとすると、領域L1は、2.4MBの容量が必要となる。第3の実施の形態では、512個のキーデータを格納するので、領域L1は4KB程度で済む。

【0082】しかも、このようにしても、演算により乱数を発生するので、セクタ毎に異なるキーデータが得られる。

【0083】図11は、本発明の第4の実施の形態の説明図、図12は、本発明の第4の実施の形態の書き込み処理フロー図である。

【0084】この第4の実施の形態は、第3の実施の形態に加えて、複数のユーザーパスワードを使用できる方法を示すものである。図11に示すように、使用者をn名まで認めるため、各使用者毎に、パスワードPW1~PWnを設定する。パスワードが8バイトであるとし

て、各使用者に対応して、8バイト（PW1の大きさ）の領域L2～Lnと、8バイトの領域C1～Cnを、光ディスク1に設ける。

【0085】記憶媒体の論理フォーマットを作成する時は、第3の実施の形態と同様に、領域L1に、乱数データをユーザーパスワードPW1により暗号化したものを書き込んでおく。

【0086】それに加えて、パスワードの検証用文字列DC1を生成し、これをパスワードPW1で暗号化したものを領域C1に書き込んでおく。更に、パスワードPW1をPW2で暗号化したものを、領域L2に書き込み、パスワードPW1をPWnで暗号化したものを、領域Lnに書き込む。

【0087】更に、パスワードPW2の検証用文字列DC2をパスワードPW2で暗号化したものを、領域C2に書き込む。以下、パスワードPWnの検証用文字列DCnをパスワードPWnで暗号化したものを、領域Cnに書き込む。

【0088】各パスワードの検証用文字列は、入力したパスワードが正しいかを検証するものである。この検証用文字列は、システムに特有の秘密の文字列で構成しても良く、パスワードPWiから計算される値（例えば、パスワードPWiとある特定の文字列との排他的論理和）としても良い。

【0089】次に、ユーザーパスワードを用いる場合のデータの書き込み、読み出し処理は、図8及び図10に示した第3の実施の形態と同様に行う。

【0090】ユーザーパスワードPWi（i>1）を用いる場合のデータの書き込みは、図12により説明する。

【0091】（S60）論理ブロックアドレス（セクタ番号）LBAが「S0」の位置への書き込み要求が生じたとする。書き込み要求する位置が、領域L1と重ならないようにするため、要求されたセクタ番号LBAを、「S1」に変更する。ここでは、図4に示したように、セクタ番号「S0」に、領域L1の大きさ「a」を加えて、変更されたセクタ番号「S1」を得る。

【0092】（S61）CPU2は、光ディスク1の領域L1のデータ（暗号化されたキーデータ）を読み出し済みを判定する。読み出し済なら、メモリ3の作業域に、キーデータが展開されているため、ステップS64に進む。

【0093】（S62）領域L1のデータが読み出し済でないなら、メモリ3の作業域に、キーデータを展開する処理を行う。即ち、CPU2は、パスワードPWiを得る。そして、領域Liを読み出し、読み出したデータをパスワードPWiで復号化する。これにより、パスワードPW1を得る。

【0094】（S63）次に、CPU2は、光ディスク1の領域L1のデータPS'〔1〕～PS'〔n〕を読

みだす。CPU2は、領域L1のデータPS'〔1〕～PS'〔n〕を、パスワードPW1で復号化する。これにより、キーデータPS〔1〕～PS〔n〕が得られる。このキーデータPS〔 〕（PS〔1〕～PS〔n〕）を、メモリ3の作業域に格納する。

【0095】（S64）CPU2は、要求されたセクタ番号S0から4つの値R0、R1、R2、R3を得る。ここでは、論理セクタ番号S0を32ビットのビット列と見なし、8ビットづつを1つの値R0、R1、R2、R3に纏める。そして、R0～R3をインデックスとして、メモリ3の作業域のPS〔 〕から乱数値（キーデータ）を取り出す。取り出した4つの値を基に、8バイトの乱数（キーデータ）Rを発生する。

【0096】ここでは、図9に示すように、R0に対応するキーデータPS〔R0〕を取り出し、（R1+256）に対応するキーデータPS〔R1+256〕を取り出す。R2に対応するキーデータPS〔R2+256〕を取り出し、R3に対応するキーデータPS〔R3〕を取り出す。

【0097】そして、上述した演算式により、キーデータRを演算する。

【0098】（S65）そして、CPU2は、書き込むべきデータを、このキーデータRで暗号化する。暗号化の方法としては、周知のDES等を用いることができる。CPU2は、この暗号化されたデータを、光ディスク1の論理ブロックアドレスLBA（=S1）の位置に書き込む。

【0099】このようにして、複数のユーザーパスワードを使用することができる。

【0100】図13は、本発明の第4の実施の形態のパスワード変更処理フロー図（その1）、図14は、本発明の第4の実施の形態のパスワード変更処理フロー図（その2）である。

【0101】図11の構成において、ユーザーパスワードPW1を変更する処理について、図13により、説明する。

【0102】（S70）CPU2は、旧パスワードPW1と新パスワードPW1'を得る。

【0103】（S71）CPU2は、光ディスク1の領域L1と領域C1を読みだす。

【0104】（S72）CPU2は、領域L1の暗号化されたキーデータを、パスワードPW1で復号化して、キーデータPS〔 〕を得る。そして、CPU2は、領域C1のデータをパスワードPW1で復号化する。更に、復号化された検証用文字列から、パスワードPW1の正当性を判定する。パスワードが正しくなければ、エラーとする。

【0105】（S73）CPU2は、キーデータPS〔 〕を、新パスワードPW1'で暗号化して、光ディスク1の領域L1に書き込む。

【0106】(S74)次に、CPU2は、新パスワードPW1'に対する検証用文字列DC1'を作成する。そして、CPU2は、検証用文字列DC1'を新パスワードPW1'で暗号化して、書き込み値C1'を得る。更に、CPU2は、書き込み値C1'を光ディスク1の領域C1に書き込む。

【0107】このようにして、旧パスワードの正当性を確認して、新パスワードに変更することができる。しかも、データの再暗号化を必要としないで、パスワードの変更ができる。この方法は、ユーザーパスワードが1つの場合に有効な方法である。

【0108】複数のユーザーパスワードを設定した場合には、図13の処理を実行して、新パスワードに変更した場合に、ユーザーパスワードPW2～PWnによるデータアクセスができなくなる。複数のユーザーパスワードを設定した場合にこれが不都合であるなら、パスワードPW1をユーザーパスワードとして使用せずに、ユーザーパスワードPW_i (i>1)のみを、使用者のパスワードとして使用すれば良い。

【0109】このユーザーパスワードPW_i (i>1) 20 を変更する処理を、図14により説明する。

【0110】(S80)CPU2は、旧パスワードPW_iと新パスワードPW_i'を得る。

【0111】(S81)CPU2は、光ディスク1の領域L_iと領域C_iを読みだす。

【0112】(S82)CPU2は、領域L_iの暗号化されたデータを、パスワードPW_iで復号化して、パスワードPW1を得る。そして、CPU2は、領域C_iのデータをパスワードPW_iで復号化する。更に、復号化された検証用文字列から、パスワードPW_iの正当性を 30 判定する。パスワードが正しくなければ、エラーとする。

【0113】(S83)CPU2は、パスワードPW1を、新パスワードPW_i'で暗号化して、光ディスク1の領域L_iに書き込む。

【0114】(S84)次に、CPU2は、新パスワードPW_i'に対する検証用文字列DC_i'を作成する。そして、CPU2は、検証用文字列DC_i'を新パスワードPW_i'で暗号化して、書き込み値C_i'を得る。更に、CPU2は、書き込み値C_i'を光ディスク1の 40 領域C_iに書き込む。

【0115】このようにして、旧パスワードPW_iの正当性を確認して、パスワードPW_iを変更できる。この例も、データの再暗号化を必要としないで、パスワードの変更が可能である。

【0116】上述の実施の態様の他に、本発明は、次のような変形が可能である。

【0117】(D) 記憶媒体を、光磁気ディスクで説明したが、光ディスク、磁気ディスク、ICカード等他の記憶媒体に適用できる。

【0118】(2) 乱数Rを求める演算式は、他の形式のものも利用できる。

【0119】以上、本発明の実施の形態により説明したが、本発明の主旨の範囲内で種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

【0120】

【発明の効果】以上説明したように、本発明によれば、次の効果を奏する。

【0121】(1) パスワードをそのまま暗号化キーとして用いるのではなく、パスワードとは、別に生成したキーデータを用いて、データを暗号化する。暗号文を解析しても、暗号化されたキーデータが解読されるだけである。このため、パスワードやキーデータを解析しにくい。これにより、暗号文の解析によるパスワードの解読を防止できる。

【0122】(2) 又、パスワードとは、別に生成したキーデータを用いて、暗号化するため、1つのパスワードに対し、キーデータを変えることにより、セクタ等の記憶単位に異なるキーを付与できる。このため、論理セクタ毎に異なるキーを用いて、暗号化でき、データの機密性を高めることができる。

【0123】(3) 更に、パスワードとは、別に生成したキーデータを用いて、暗号化するため、パスワードを変えても、データの再暗号化が不要となる。このため、数百メガバイトの大容量記憶媒体でも、容易にパスワードの変更を実現できる。

【図面の簡単な説明】

【図1】本発明の一実施の形態のブロック図である。

【図2】本発明の第1の実施の形態の論理フォーマット時の処理フロー図である。

【図3】本発明の第1の実施の形態の書き込み処理フロー図である。

【図4】本発明の第1の実施の形態の記憶領域の説明図である。

【図5】本発明の第1の実施の形態のキーデータの説明図である。

【図6】本発明の第1の実施の形態の読み出し処理フロー図である。

【図7】本発明の第2の実施の形態の書き込み処理フロー図である。

【図8】本発明の第3の実施の形態の書き込み処理フロー図である。

【図9】本発明の第3の実施の形態のキーデータの説明図である。

【図10】本発明の第3の実施の形態の読み出し処理フロー図である。

【図11】本発明の第4の実施の形態の説明図である。

【図12】本発明の第4の実施の形態の書き込み処理フロー図である。

50 【図13】本発明の第4の実施の形態のパスワード変更

17

処理フロー図（その 1）である。

【図 1 4】 本発明の第 4 の実施の形態のパスワード変更
処理フロー図（その 2）である。

【図 1 5】 従来技術の説明図である。

【符号の説明】

1 光ディスク（記憶媒体）

*

* 2 制御回路（CPU）

3 メモリ

20 第 1 の暗号化部

21 第 2 の暗号化部

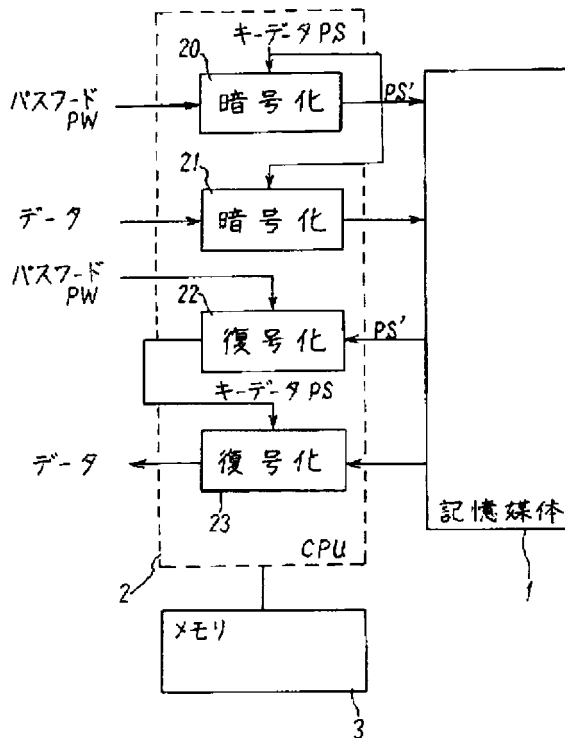
22 第 1 の復号化部

* 23 第 2 の復号化部

18

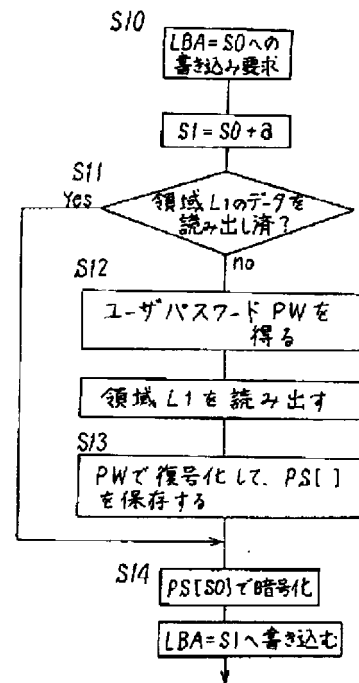
【図 1】

ブロック図



【図 3】

書き込み処理フロー図

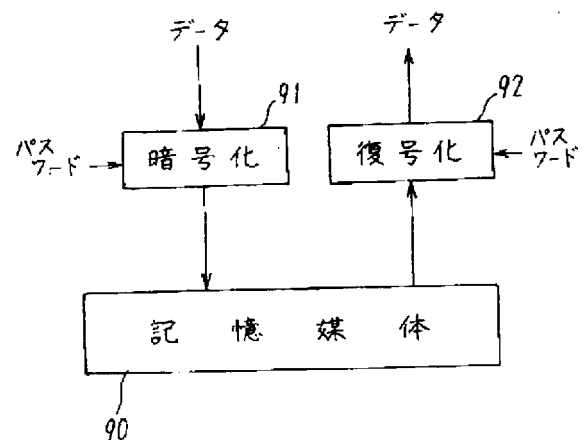
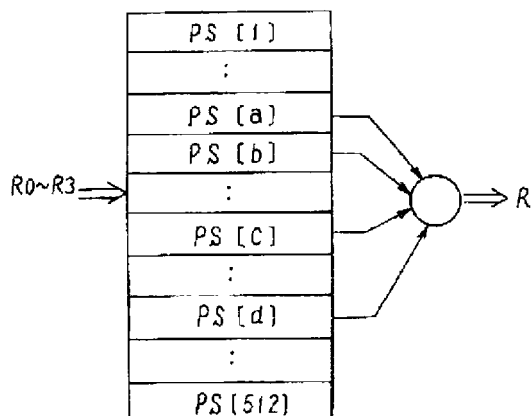


【図 1 5】

従来技術の説明図

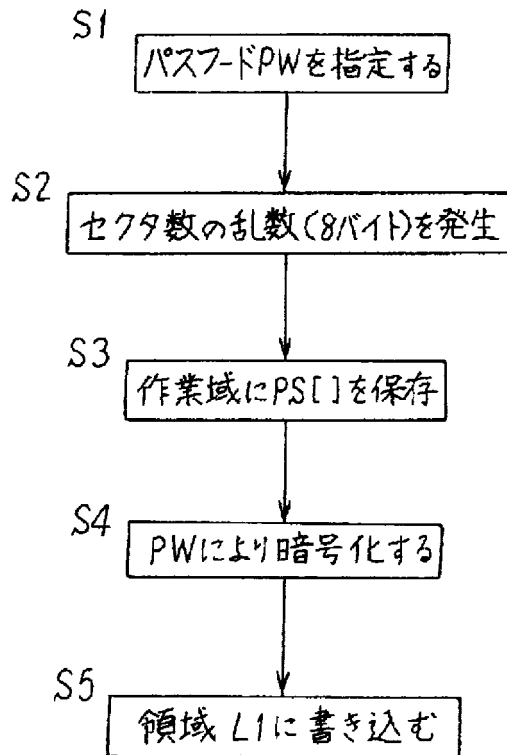
【図 9】

キーデータの説明図



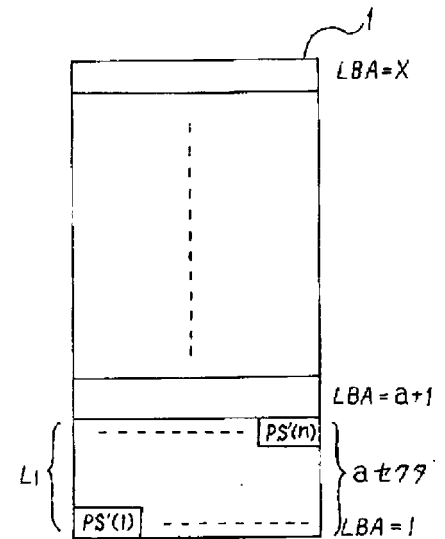
【図2】

論理フォーマット時の処理フロー図



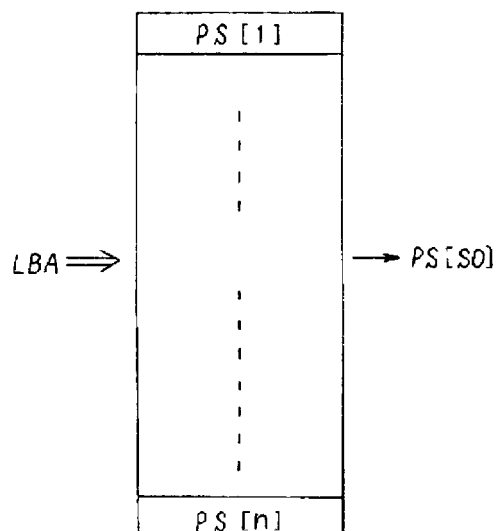
【図4】

記憶領域の説明図



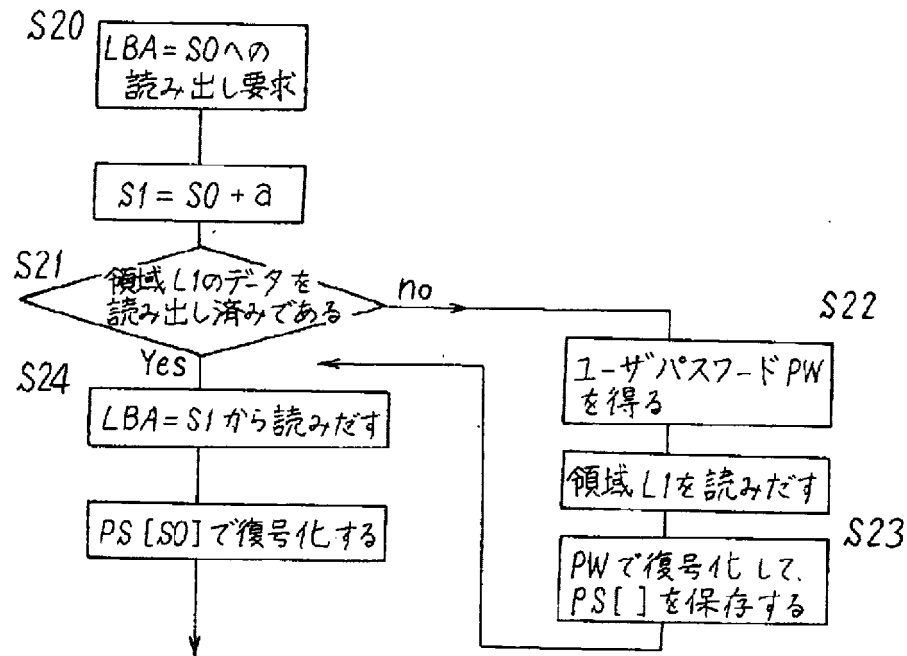
【図5】

キーデータの説明図



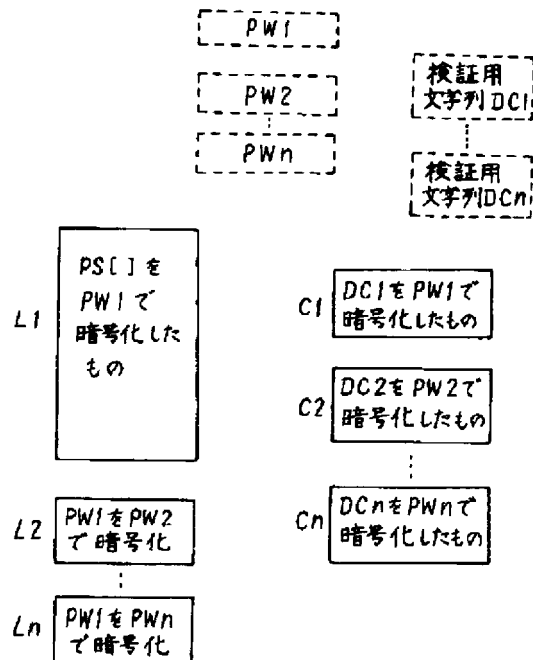
【図6】

読み出し処理フロー図



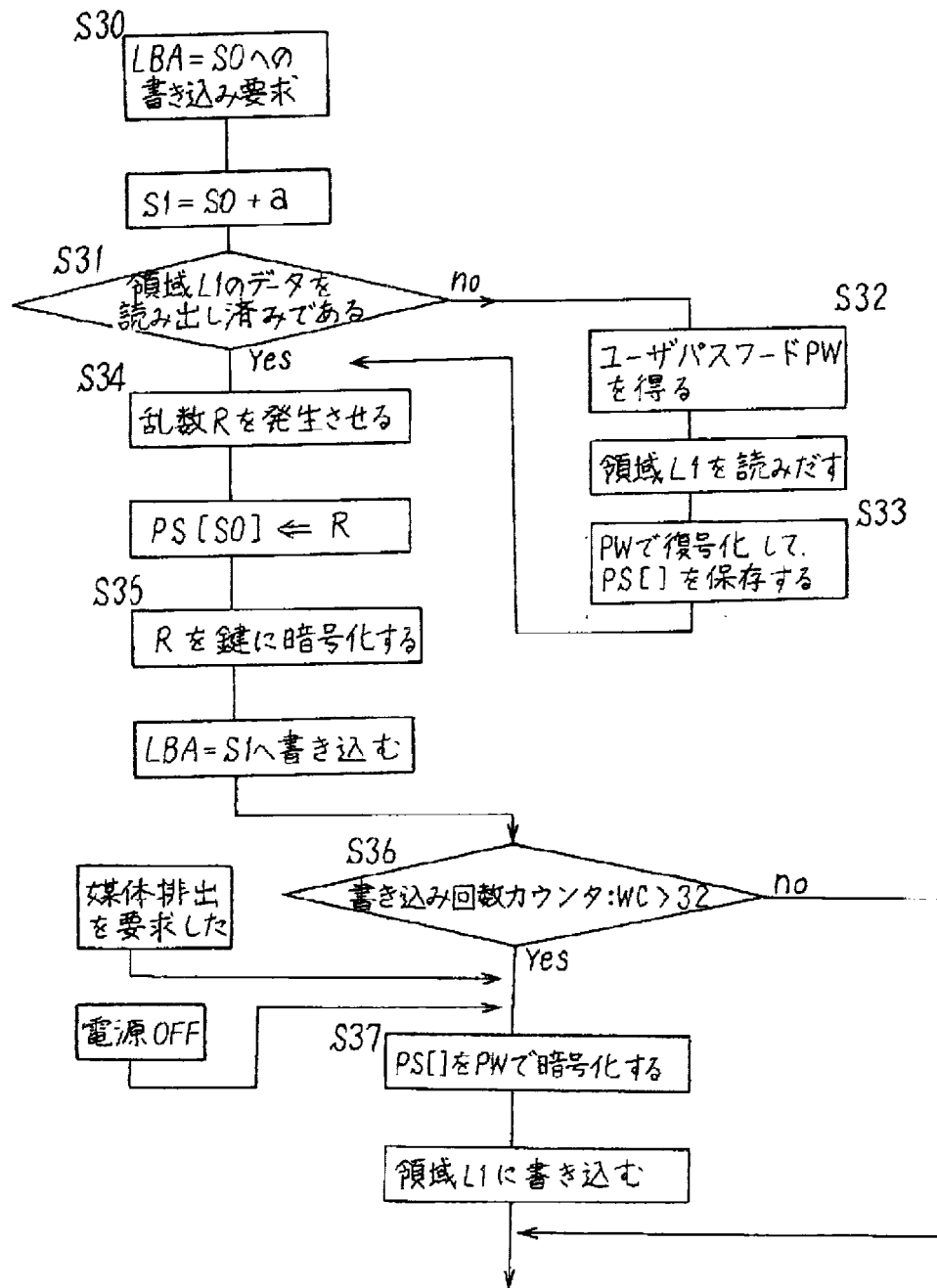
【図11】

第4の実施の形態の説明図



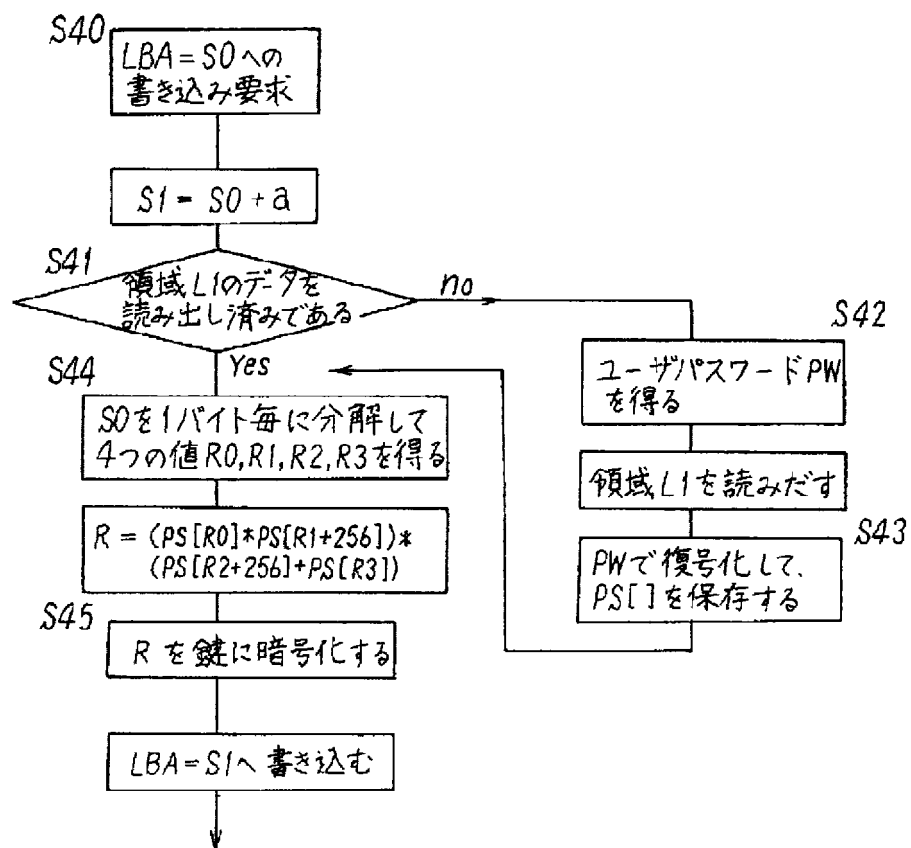
【図7】

書き込み処理フロー図



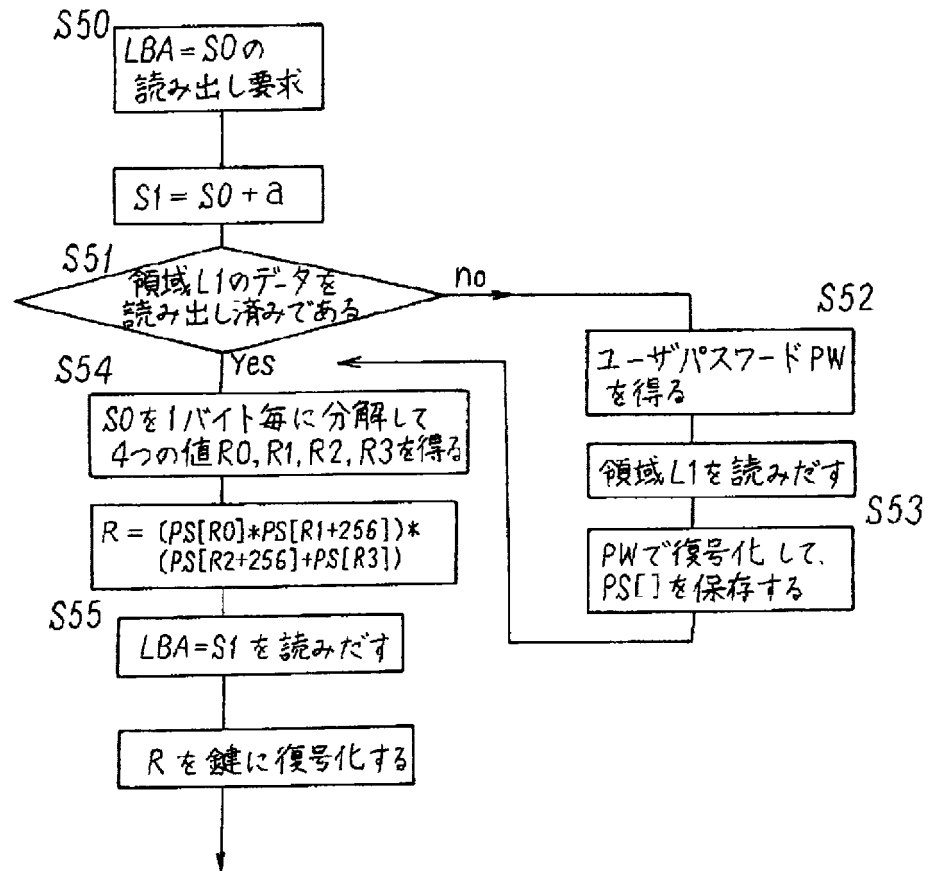
【図8】

書き込み処理フロー図



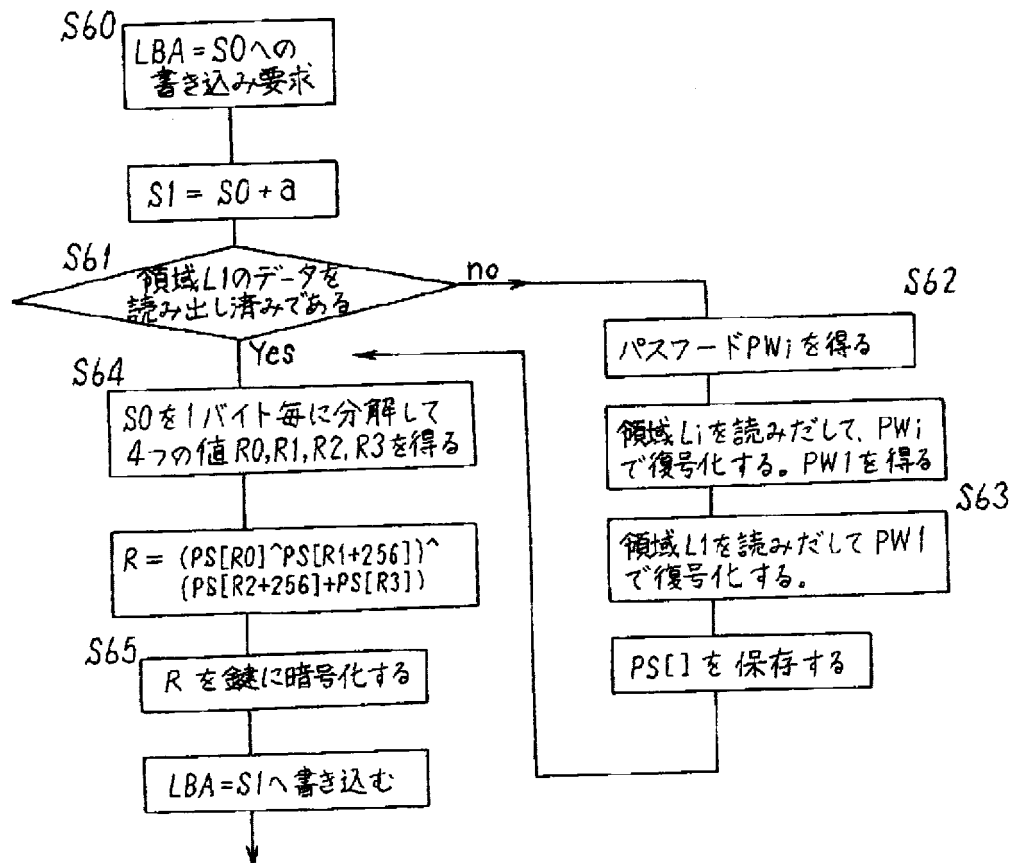
【図10】

読み出し処理フロー図



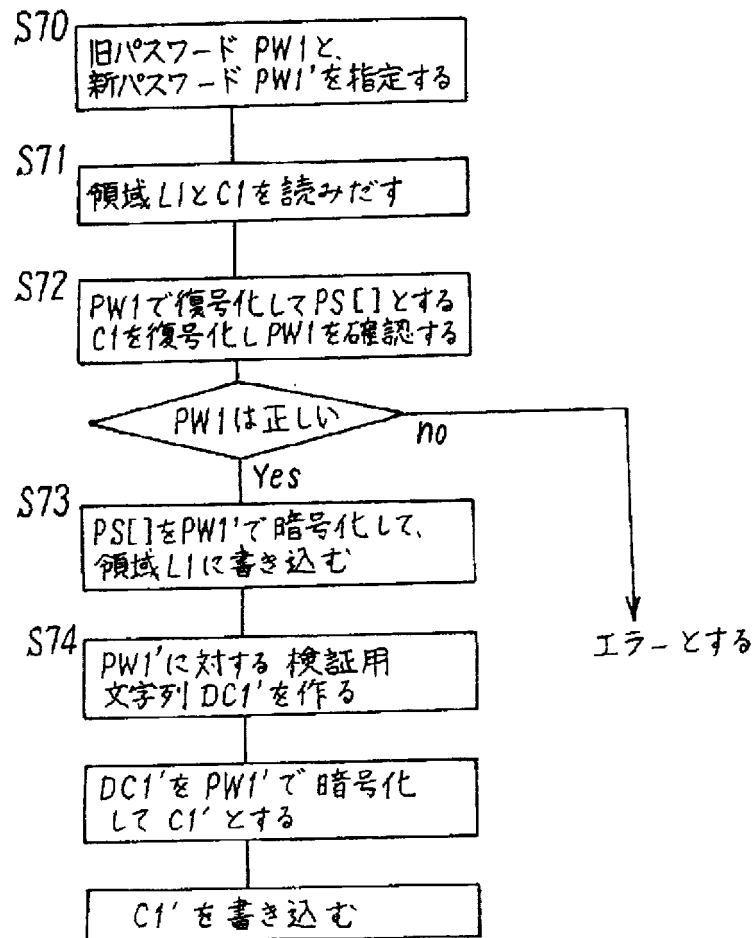
【図 1 2】

書き込み処理フロー図



【図13】

パスワード変更処理フロー図(その1)



【図 1 4】

パスワード変更処理フロー図(その2)

